Differential Cryptanalysis of Round-Reduced PRINTCIPHER: Computing Roots of Permutations

Mohamed Abdelraheem, Gregor Leander and Erik Zenner

DTU Mathematics

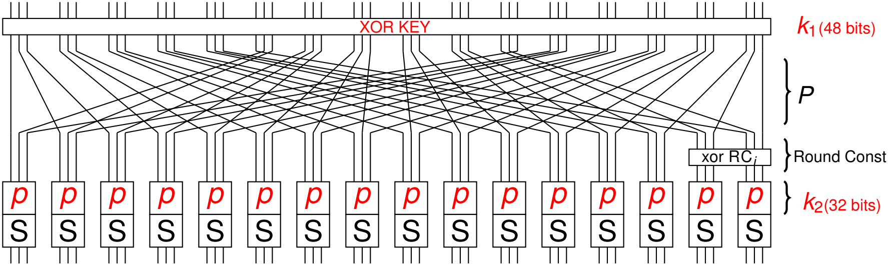
FSE 2011

Outline

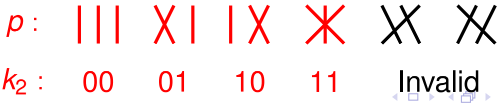
Introduction

- PRINTcipher is a lightweight SPN block cipher proposed at CHES 2010.
- Two versions: PRINTcipher-48 and PRINTcipher-96.
- Focus on PRINTcipher-48.

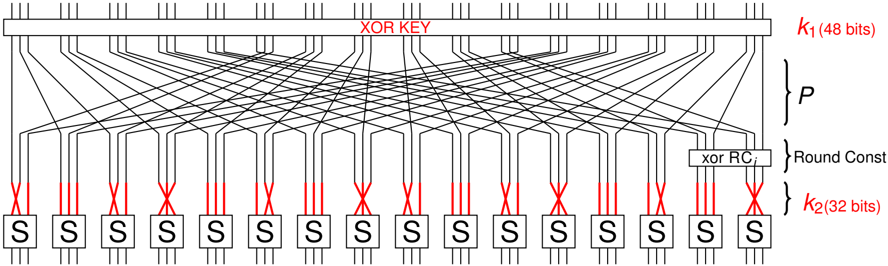
One round of PRINTCIPHER-48



- 48-bits block size, 48 rounds that use the same 80-bit key.
- Each two bits of k_2 permute 3 state bits in a certain way.
- Only 4 out of 6 possible permutations are allowed:



Example showing how k_2 is used

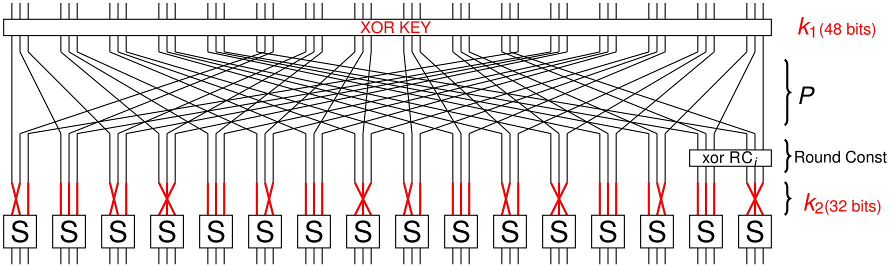


$$k_2 = 01,00,01,11,00,10,00,11,01,00,01,11,00,10,00,11$$

p :

k_2 : 00 01 10 11

P and $k_2 \in S_{48}$



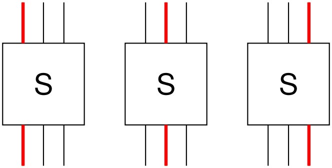
- k_2 = 01, 00, $\cdots$, 11.
- $k_2 \in S_{48} : (1,2)(3)(4)(5)(6)\cdots(46,48)(47)$.
- $P \in S_{48}$, $P(i) = (3i-2) \mod 47, P(48) = 48$.
- $P = (1)(2,4,10,\cdots,17)(6,16,46,\cdots,34)(48)$.
- Linear layer is key-dependent.

Outline

Differential Characteristics

- $Pr(\Delta X \rightarrow \Delta Y) = \{0, \frac{1}{4}\}$.
- So r-round characteristics have prob. $\leq (\frac{1}{4})^r$.
- Problem: key dependent linear layer.

Optimal Characteristic

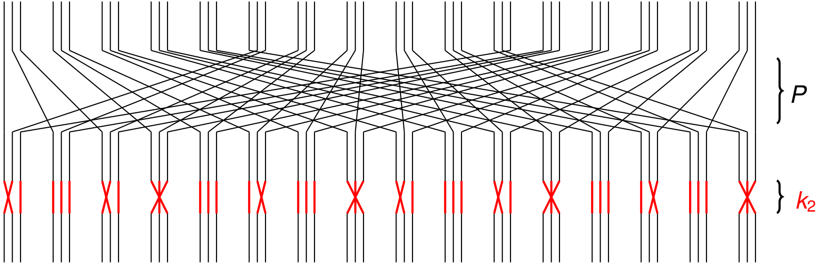


$$\Delta x = \Delta y \text{ with Pr} = \frac{1}{4}$$

For any 1-bit input difference:

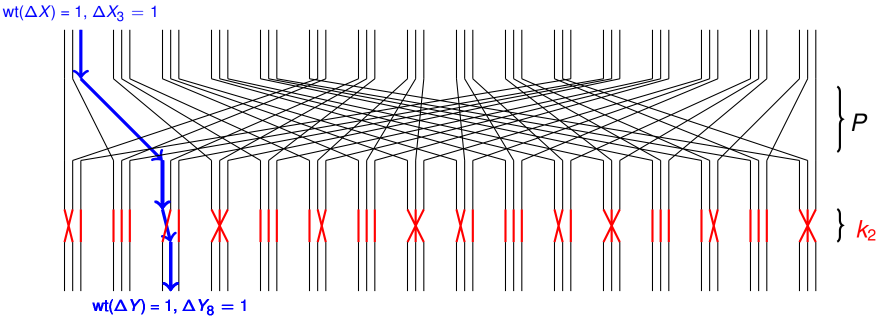
- Only one active Sbox in each round is possible.
- Unique optimal characertisic with Pr = $\frac{1}{4^r}$ for r rounds.

Differential on one round of PRINTcipher



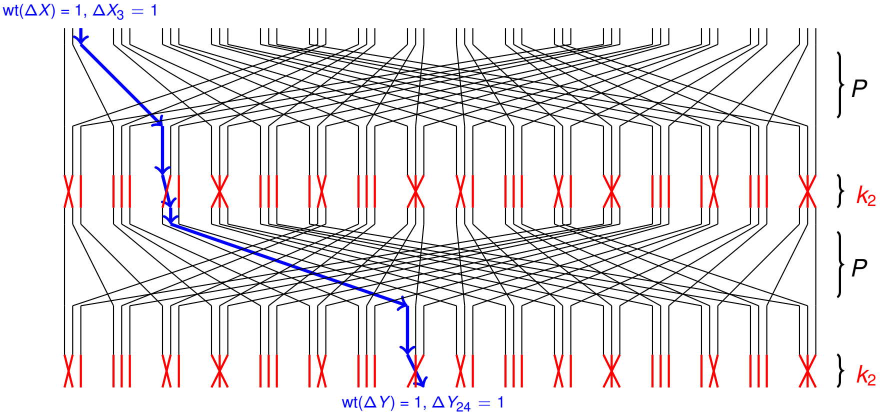
- No xor key.
- No RC.
- No Sboxes.
- Only the linear layer $\equiv$ composition of P and $k_2 = P \circ k_2 = Pk_2$.

Differential trail on one round of PRINTcipher



- $Pk_2(3) = 8$.
- By trying all the 48 1-bit input differences: we learn Pk_2 .

Differential on two rounds of PRINTCIPHER



- Composition of permutations: $(Pk_2) \circ (Pk_2) = (Pk_2)^2$.
- We learn that $(Pk_2)^2(3) = 24$.

Differential Cryptanalysis of r rounds:

If we have a 1-bit difference at position i, then after r rounds:

- We learn that $(Pk_2)^r(i) = j$.
- Trying all i's: we learn $(Pk_2)^r$.
- Works only for $r \leq 22$ using the full code book.
- Finding k_2 is now reduced to computing the r-th roots of $(Pk_2)^r$.

Outline

Computing roots of permutations

- **Problem:** Given σ^r, find σ.
- **Solution:** Compute the r-th roots of the permutation σ.
- Computing roots of permutations is easy.
- **Problem:** There could be many roots for σ.
  - σ^{22} = Identity, has $\approx 2^{192}$ roots, so it is inefficient to find them all.
  - Almost all of them are not of the form Pk_2 .
- **Solution:** Find only those roots which are valid for PRINTCIPHER by using known algorithms and exploiting the structure of Pk_2.

Pk_2 structure 1

For $1 \leq i \leq 16$:

- When applying P, the 3-bits i, $i + 16$ and $i + 32$ go to the ith Sbox.
- Then they are permuted according to k_2 before entering the Sboxes.

Pk_2 structure 2

For all $1 \leq i \leq 48$:

- **Property 1**: $Pk_2(i)$ equals one of the following three possible values depending on k_2,

$$Pk_2(i) = \begin{cases} 3i - 2 \pmod{48} \\ 3i - 1 \pmod{48} \\ 3i \pmod{48} \end{cases}$$

- **Property 2**: Only 4 out of the 6 possible 3-bit permutations are valid. So the following cannot hold:
  - $Pk_2(i) = 3i - 1$, $Pk_2(i + 16) = 3i$ and $Pk_2(i + 32) = 3i - 2$.

  - $Pk_2(i) = 3i$, $Pk_2(i + 16) = 3i - 2$ and $Pk_2(i + 32) = 3i - 1$.

Experimental results

- $(Pk_2)^r$ has only one PRINTCIPHER root for most keys.
- Tried 2^{13} random k_2 values for different number of rounds:
  - When $r = 22$, only $2^{9.6}$ keys yield more than one root.
  - Took few seconds on average.
- Worst case is when $(Pk_2)^r$= Identity.
  - When $r = 22$, it took less than 3 hours and there are $\approx 2^{22}$ roots $\approx 0.1\%$ of all possible k_2.

Outline

Summary

- Attacked 22/48 rounds of PRINTCIPHER-48 using the full code book.
- The key-dependent linear layer of PRINTCIPHER adds no security against differential cryptanalysis.
- Recovered the key-dependent linear layer by: computing roots of permutations in S_{48}.

Thank you for your attention